BY ORDER OF THE COMMANDER
TRAVIS AIR FORCE BASE

TRAVIS AFB INSTRUCTION 33-101

19 MAY 1995

Command, Control, Communications, and
Computer (C4) Systems

SMALL COMPUTER MANAGEMENT

COMPLIANCE WITH THIS PUBLICATION IS MANDATORY

NOTICE: This publication is available digitally on the AFDPO/PP WWW site at: **http://afpubs.hq.af.mil.**

OPR: 60 CS/SCUS (TSgt Daniel J. Negrillo)
Supersedes 60 AMWR 700-19, 30 October 1994

Certified by: 60 CS/CCQ (Lt Eric S. Bulger)
Pages: 6
Distribution: F

This instruction implements AFPD 33-1, *Command, Control, Communications, and Computer (C4) Systems*. It outlines responsibilities for the complete management of small computer resources including hardware/software acquisition and accountability, computer security, maintenance, training, networking, and Emission Security (Formerly TEMPEST) requirements pursuant to Automated Data Processing Equipment (ADPE). This instruction describes responsibilities of the 60th Communications Squadron and mandates responsibilities of the Computer System Manager (CSM) for all base units.

SUMMARY OF REVISIONS

Changes 60th Airlift Wing (60 AW) to 60th Air Mobility Wing (60 AMW), 60th Communications Group (60 CG) to 60th Communications Squadron (60 CS), References, Computer Facility Manager (CFP) to Computer System Manager (CSM), and redefines 60 CS responsibilities.

1. REFERENCES:

1.1. AFI 33-103, Requirements Developing and Processing

1.2. AFI 33-112, Automated Data Processing Equipment Management

1.3. AFI 33-115, Network Management

1.4. AFI 33-202, Air Force Computer Security Program

1.5. AFI 33-203, Air Force TEMPEST Program

1.6. AFI 33-204, C4 Systems Security Awareness, Training, and Education (SATE) Program

1.7. AFI 33-218, TEMPEST Protection

2. APPOINTMENT OF COMPUTER SYSTEM MANAGER (CSM):

2.1. Each unit commander will appoint, in writing, a primary and an appropriate number of alternate CSMs. Each unit commander will ensure appointments and responsibilities are transferred 45 days prior to appointees being relieved of duty, reassigned, placed on TDY exceeding 45 days, or scheduled to separate. These individuals will be computer literate and will have adequate time to accomplish their duties, as outlined in this instruction and the references above.

2.2. CSMs will be responsible for managing the following areas: Computer Security (COMPUSEC), Emission Security (Formerly TEMPEST), organizational small computer management, equipment accountability, hardware/software acquisition, network management, and training.

3. GENERAL RESPONSIBILITIES OF CSM:

3.1. Ensure equipment inventory of ADPE no later than 31 March annually.

3.2. Ensure contingency/backup plans are in place and documented for mission essential computer systems.

3.3. Ensure security incidents are reported to the appropriate agencies.

3.4. Take necessary actions to plan for all future computer hardware/software requirements.

3.5. Ensure basic hardware/software troubleshooting is accomplished prior to contacting the 60th CS Help Desk.

3.6. Control access to computer assets including hardware, software, and stored data guaranteeing computer use is in compliance with Air Force, MAJCOM, and base directives.

3.7. Establish and maintain a current small computer library consisting of applicable directives for use as a unit reference point.

3.8. Attend or send alternate(s) to periodic CSM meetings.

3.9. Be responsible for accepting delivery of ADPE hardware/software including completion of accreditation packages.

3.10. Load anti-virus software on all computer systems and report any identified virus incidents.

3.11. Ensure computer software is used within the established commercial licensing agreements.

4. SPECIFIC RESPONSIBILITIES OF CSM:

4.1. COMPUSEC:

4.1.1. Appoint, in writing, an adequate number of Computer System Security Officers (CSSOs) to implement the COMPUSEC program in their respective areas.

4.1.2. Ensure stand alone classified computer systems and local area networks (LANs) under their control are accredited prior to system operation.

4.2. EMISSION SECURITY:

4.2.1. Contact the Base Emission Security Manager for assistance as soon as it is determined classified information will be processed.

4.2.2. A primary and alternate unit emission security monitor must be appointed in writing if classified information is processed on a computer system.

4.2.3. At the earliest date possible, and before classified information is processed, request the Base Emission Security Manager perform a countermeasure assessment.

4.3. ORGANIZATIONAL SMALL COMPUTER MANAGEMENT:

4.3.1. Assume duties or appoint, in writing, a primary and alternate Organizational Small Computer Manager (OSCM).

4.3.2. Identify all excess computer software assets for reutilization. Final disposition of non-reutilized excess software will be determined by the 60 CS Small Computer Support Office.

4.3.3. Attempt to reallocate excess software within your organization.

4.4. EQUIPMENT CUSTODIAN (EC):

4.4.1. Appoint, in writing, a primary and an alternate EC.

4.4.2. Maintain accountability of all ADPE assets.

4.4.3. Identify all excess computer hardware assets to the 60 CS Equipment Control Officer (ECO) for disposition instructions.

4.5. HARDWARE/SOFTWARE ACQUISITION:

4.5.1. CSMs will ensure requirements for new hardware/software are researched, documented, and justified.

4.5.2. Coordinate with the 60 CS ECO for possible acquisition of alternate resources in lieu of new purchases.

4.5.3. Submit documentation of all ADPE acquisitions and coordinate through the 60 CS Computer Requirements Office.

4.5.4. Ensure appropriate coded money (3400 vs 3080) is used when purchasing computer assets.

4.6. NETWORK MANAGEMENT:

4.6.1. Assume duties or appoint, in writing, a primary and alternate as Network Manager and Network Security Manager.

4.6.2. Ensure that a network security plan has been accomplished and documented.

4.6.3. Coordinate and update network blueprints with the Base Network Control Center (BNCC).

4.6.4. Ensure contingency/backup plans are in place and documented for network servers and gateways.

4.6.5. Quarterly, perform random tests of network security features, (i.e. trustee directory assignment rights, password verification, etc.), and document and report deficiencies to the BNCC.

4.6.6. Provide network familiarization training to end users.

4.6.7. Ensure network modifications are coordinated through the Designated Approving Authority (DAA).

4.7. TRAINING:

4.7.1. Within 30 days of appointment, CSMs will ensure the successful completion and documentation of the following mandatory training:

4.7.1.1. PC-based Security Awareness, Training and Education (SATE) program tutorials for all personnel.

4.7.1.2. Basic troubleshooting techniques for CSM, OSCM, and LAN Managers as applicable.

5. RESPONSIBILITIES OF THE 60TH COMMUNICATIONS SQUADRON:

5.1. General:

5.1.1. Provide initial and/or recurring training to CSMs for each area of responsibility.

5.1.2. Act as liaison between base level organizations and MAJCOM agencies.

5.1.3. Conduct periodic CSM meetings.

5.1.4. Provide advice and guidance to the CSMs.

5.2. Base C4 Systems Security Office (BC4SSO) will:

5.2.1. Administer the COMPUSEC, Emission Security, and Security Awareness, Training, and Education (SATE) Programs.

5.2.2. Act as accreditation advisor to the DAA.

5.2.3. Review locally conducted risk analyses and recommend approval or disapproval of accreditation requests to the appropriate DAA.

5.2.4. Distribute the Air Force antiviral product.

5.2.5. Conduct initial emission security countermeasure assessments on all C4 and other facilities, systems, and equipment before processing classified information.

5.3. Base Small Computer/Secure Systems Technical Center will:

5.3.1. Repair small computer assets using a combination of blue suit and contractor maintenance after initial unit trouble-shooting efforts have been exhausted.

5.3.2. Maintain all blanket purchase agreements for contractor maintenance.

5.3.3. Maintain excess software for base reutilization.

5.3.4. Provide hardware/software consultation for small computer system upgrade and procurement.

5.4. Base Network Control Center (BNCC) will:

5.4.1. Coordinate on and process all Computer System Requirement Documents (CSRDs) for LAN Procurement.

5.4.2. Provide hardware/software compatibility consultation for procurement planning and implementation of LANs.

5.4.3. Provide a 24 hour point of contact to assist CSMs in troubleshooting computer system and LAN problems and to forward repair requests to the proper office.

5.5. Base Computer Requirements Office will:

5.5.1. Coordinate on and process all CSRDs.

5.5.2. Review all ADPE acquisition requirements and approve or validate based on fiscal limits.

5.5.3. Coordinate documentation with the CSM for the disposition of excess ADPE.

5.5.4. Maintain master Information Processing Management System (IPMS) database.

5.5.5. Accept and distribute to CSMs all computer assets delivered to the base.

DOLORES M. OSBORNE-HENSLEY, Capt, USAF
Chief, Base Information Management

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

AFI 33-103, Requirements Developing and Processing

AFI 33-112, Automated Data Processing Equipment Management

AFI 33-115, Network Management

AFI 33-202, Air Force Computer Security Program

AFI 33-203, Air Force TEMPEST Program

AFI 33-204, C4 Systems Security Awareness, Training, and Education (SATE) Program

AFI 33-218, TEMPEST Protection